



Major Murry Moskowitz
Defense Information Systems Agency
Deputy HLS C2 ACTD Program Manager
April 18, 2002



“9/11”

Phone lines jammed after attacks

BY MICHAEL DAVIS AND
VANDANA SINHA
THE VIRGINIAN-PILOT

Tuesday's terrorist attacks in New York and Washington prompted a barrage of telephone calls to and from the region, overloading the East Coast's communications grid and jamming phone and wireless services across Hampton Roads for much of the day.

"It was like the phone couldn't tell I was dialing. Then I got a fast busy signal," said Chesapeake resi-

sites of graphics and advertisements, hoping that would speed up traffic.

Local news sites were hardly spared.

"The WVEC Web site is getting an inordinately high amount of traffic," said Ralph A. Rogers, general manager of Exis Net Inc., which hosts the site. "It's probably three to five times more than we'd normally see."

With double the normal number of site visits, **pilot-online.com** juggled content between three servers. By 2

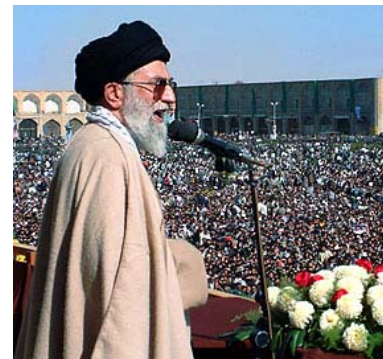
Local consumers found that many phone calls failed to go through or were dropped. For at least part of the morning, South Hampton Roads could not reliably connect to the Peninsula, although traffic eased as the day progressed.

"We're doing our best, but something of this magnitude you just can't plan for," said Scott E. Golden of Cavalier Telephone, which has about 40,000 land-line customers around Hampton Roads.

Wireless services such as cellular phones and pagers

✓ **Voice and Data Communications Interrupted**

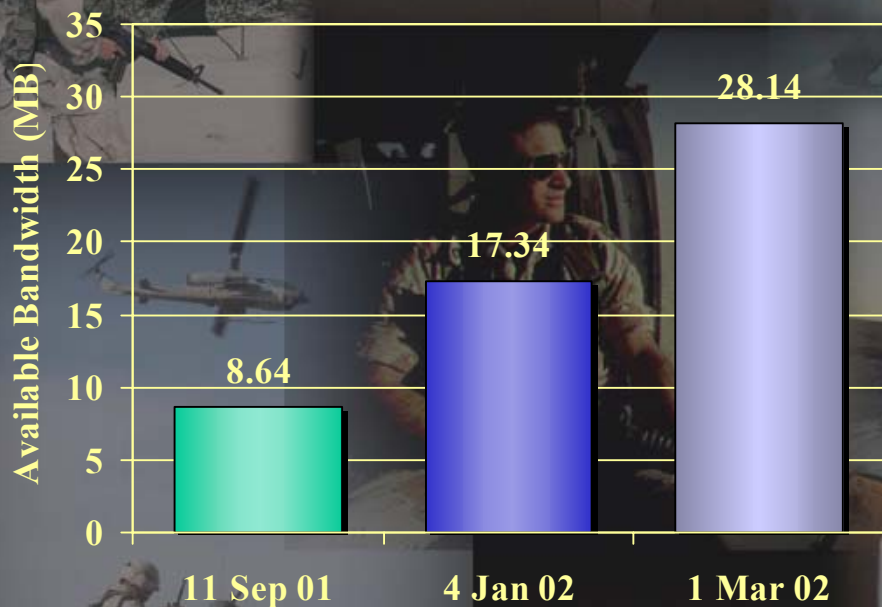
✓ **Degraded Command, Control, and Coordination**





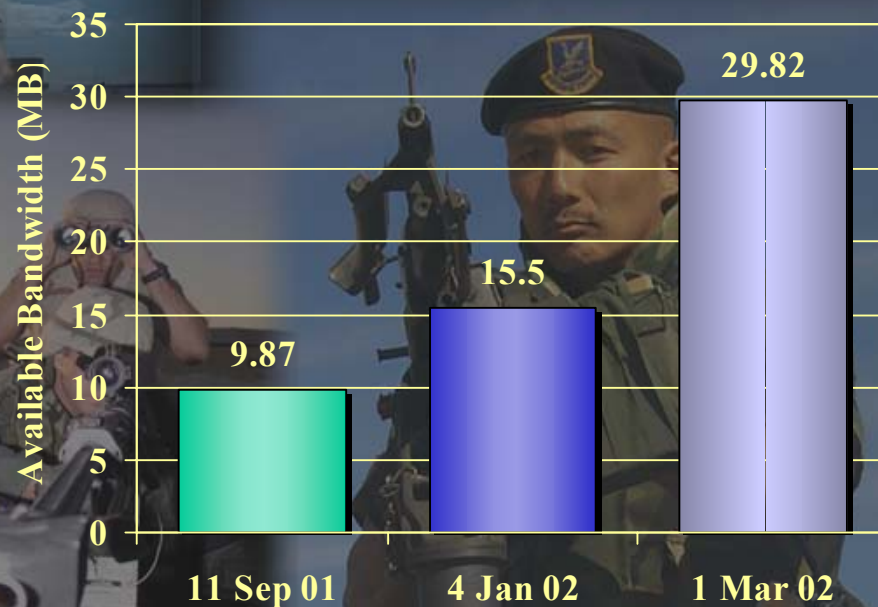
Increasing Bandwidth in Southwest Asia

NIPRNET



**226% Increase
in Bandwidth!**

SIPRNET



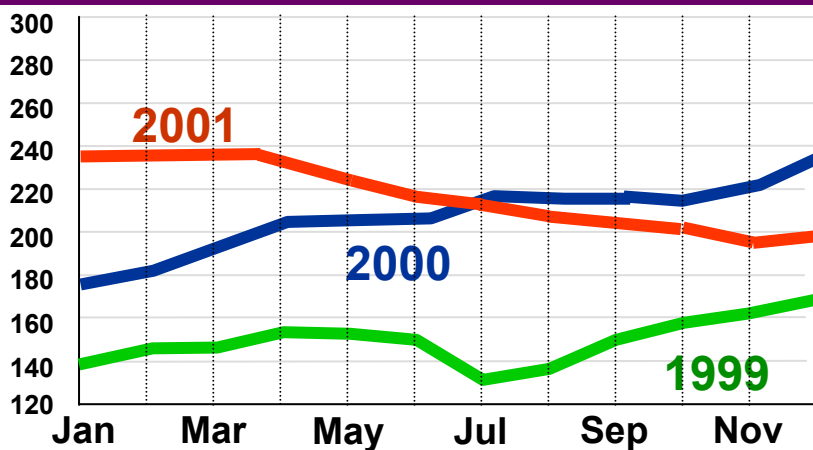
**200% Increase
in Bandwidth!**

“The No. 1 technology challenge facing warfighters in Afghanistan is the need for more bandwidth.” - Maj Gen Croom, JS/VJ6

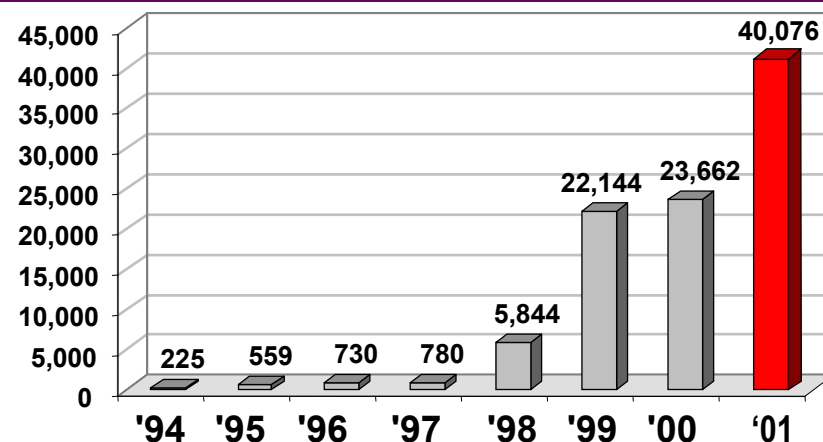


Malicious Activity Continues to Climb

Virus Growth Per Month (Internet - "Wild List")



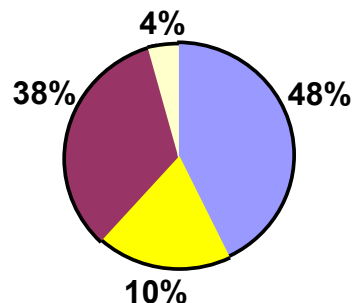
Detected "Events" (DoD Unclassified Network "NIPRNet")



"Information Networks must be controlled, protected, and managed as effectively as weapon systems."

**Lt Gen Harry D. Raduege,
DISA Director**

492 Unauthorized DoD Root-Level Intrusions (as of 31 Dec 01)

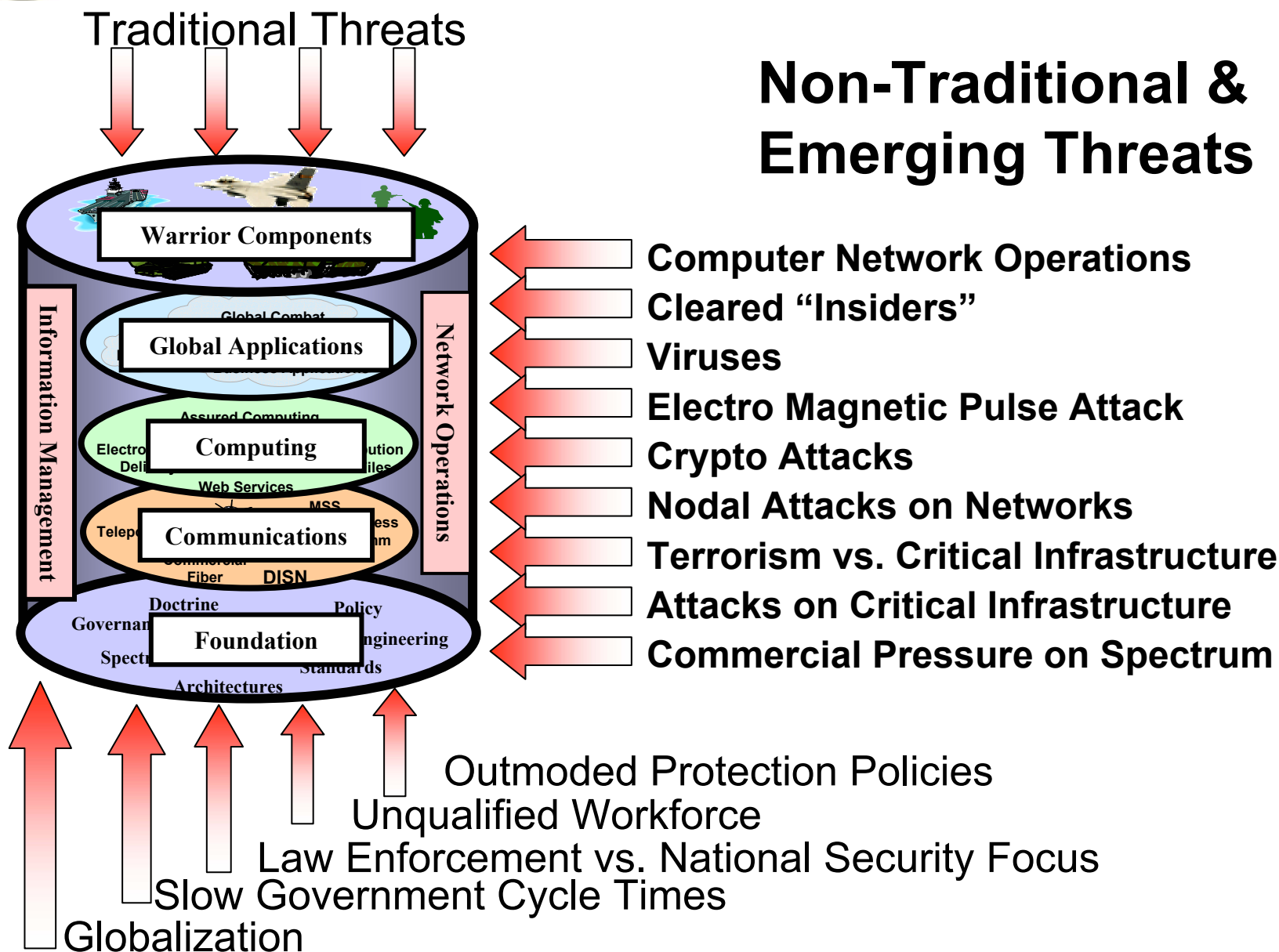


96% Preventable

- IAVA/ Bulletins
- "Multiple Vulnerabilities"
- "New" Intrusion Method or Under Analysis
- "Multiple Vulnerabilities"



Threats to the Global Information Grid





GIG Bandwidth Expansion Benefits

Supports the war on terrorism and transformation of US defense by providing survivable, critical network foundation that enables worldwide network-centric operations

- **Ensures that critical GIG C2 infrastructure has sufficient bandwidth with physical diversity**
 - Provides a minimum four-fold increase in access bandwidth capacity
 - Eliminates single points of failure
- **Fully supports DoD's continuing investments in surveillance capabilities, such as Global Hawk, reachback, sensor-to-shooter integration, collaboration, and enterprise computing**



HLS C2 ACTD

History:

- **Pre-dates “911” Attacks**
- **Submitted as Candidate in Feb 2001**
- **Approved for FY02 Start**
- **Program only 14-weeks Old**

Problem Statement

Nation needs an assured, secure, survivable multi-agency network infrastructure and IT environment for HLS across DoD, federal, state, local govts, and civil authorities



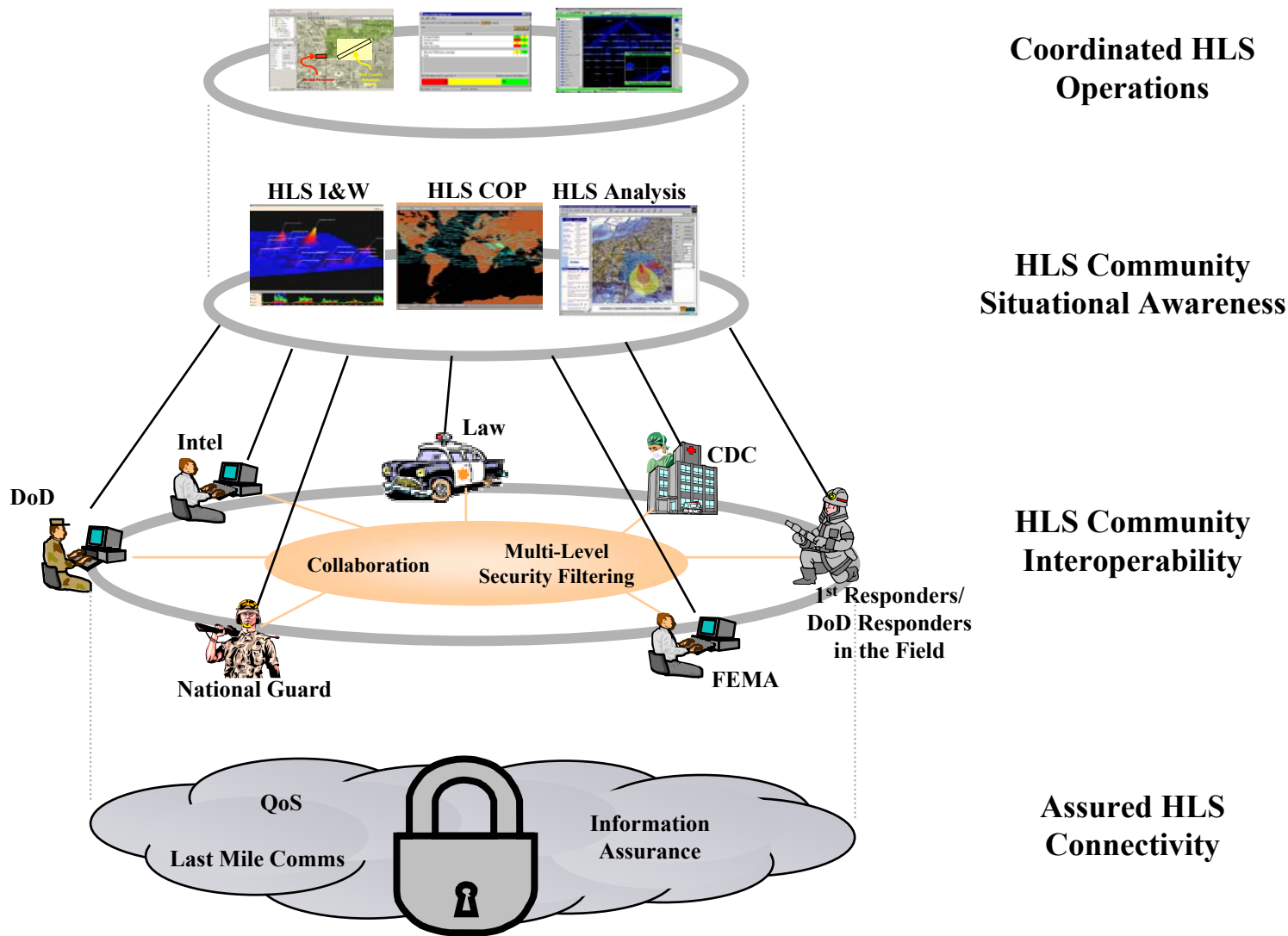
The ACTD - Three Thrust Areas

1. **ASSURED CONNECTIVITY**: Preserve the ability to coordinate federal, state, and local activities during periods of high network disruption
2. **THREAT ATTRIBUTION**: Capability to assess and track the threat across multiple information domains; and provide high-confidence, timely alerts
3. **COMMAND, CONTROL, COORDINATION**: Provide coordinated response to contain/neutralize threats and recover from damage



HLS Communities of Interest and Response Continuum

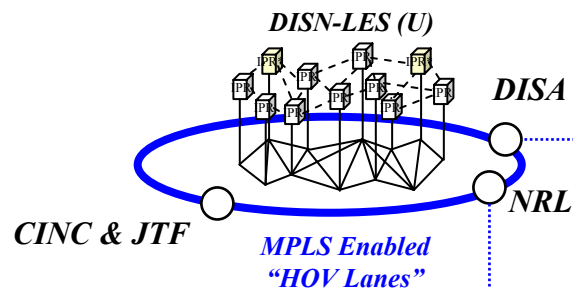
Prevention Deterrence Crisis Response Attribution



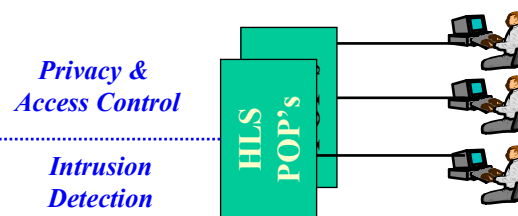


Assured Connectivity

Core Communications (MPLS backbone)

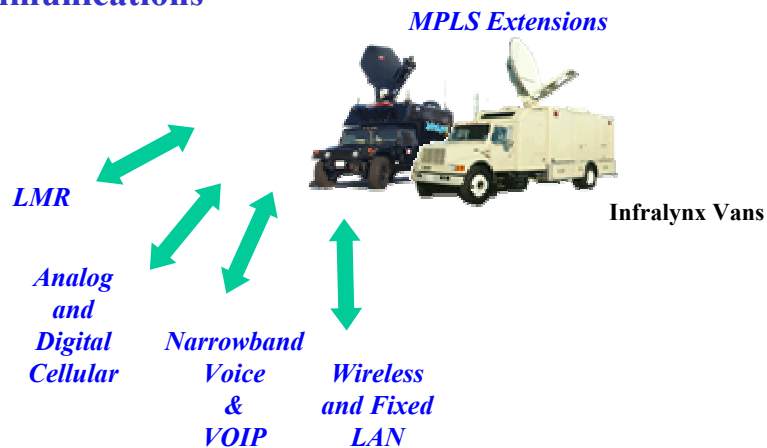


Privacy and Access Control Services



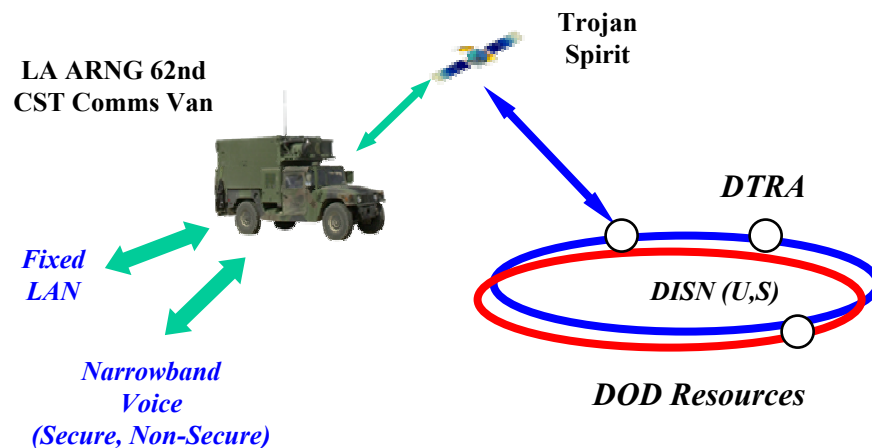
LS State EOP
LA State Police
Chesapeake EOC

Broadband Extension of Core Communications



JTF responders (LA, VA)

Reachback DOD Communications



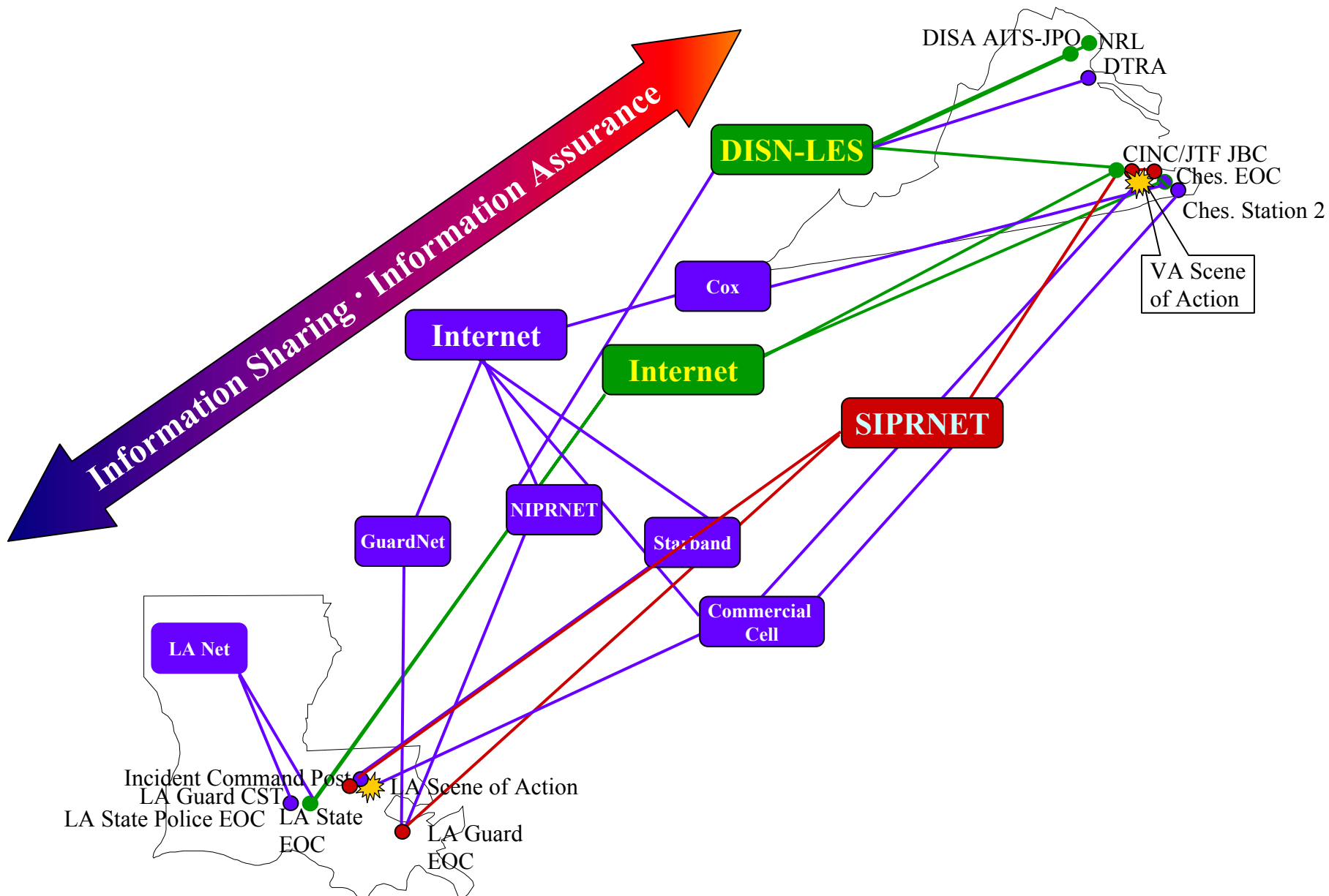
LA Army National Guard Support to Incident Commander (62nd CST)

VA CST will be present in Chesapeake



Crisis Response Demonstration

April 24-25, 2002





CONCLUSION

THE CHALLENGE

TO MODEL NETWORKS COMPRISED OF SATTELITE, WIRELESS AND IP LINKS IN ORDER TO TEST SOLUTIONS THAT CAN:

- 1. WITHSTAND CYBER ATTACKS OVER SECURE AND UNSECURE NETWORKS**
- 2. ENSURE LOW LATENCY, LOW JITTER, END-TO-END USER TRAFFIC (VoIP, DATA, VIDEO) DURING PERIODS OF PEAK CONGESTION AND DISRUPTION**